明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

資料7−2−1

情報流通の健全化
～サイバーセキュリティの観点から～

2024/1/25

情報セキュリティ大学院大学
後藤 厚宏

デジタル空間における情報流通の課題

第1回検討会での後藤メモより

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 巧妙な偽・誤情報の生成・拡散

⇒リスク増に伴い、情報やデータの「トラスト」を得る（確認する）ためのコスト増

⇒社会活動（個人・コミュニティ・企業他）の「質」の劣化・効率劣化

⇒選挙介入や安全保障上の課題への対処も必要に

- 欧州DSA– Digital Services Actの最初の適用（4カ月前倒し）がIsrael–Hamas紛争対応

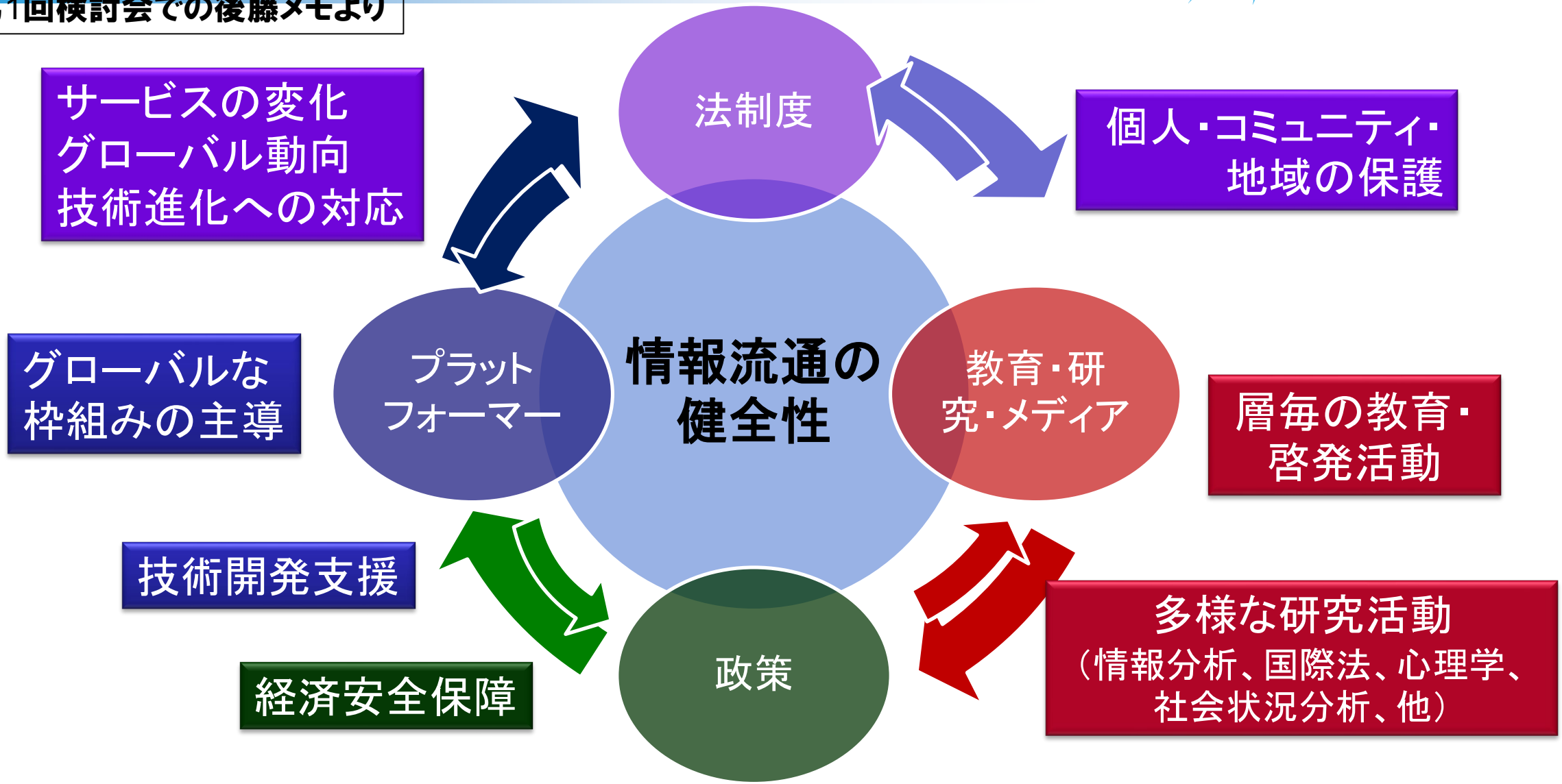
■ 社会の変化（サービス、技術、教育、・・・）に対応し（できれば将来変化を先取りし）取組みの継続が必要。

⇒多角的かつスパイラル的に取組を継続する社会的な仕組み作りが重要

（サイバーセキュリティ対策と同じく長期戦）

偽情報・誤情報対策：多様な取組みをスパイラル的に継続

第1回検討会での後藤メモより



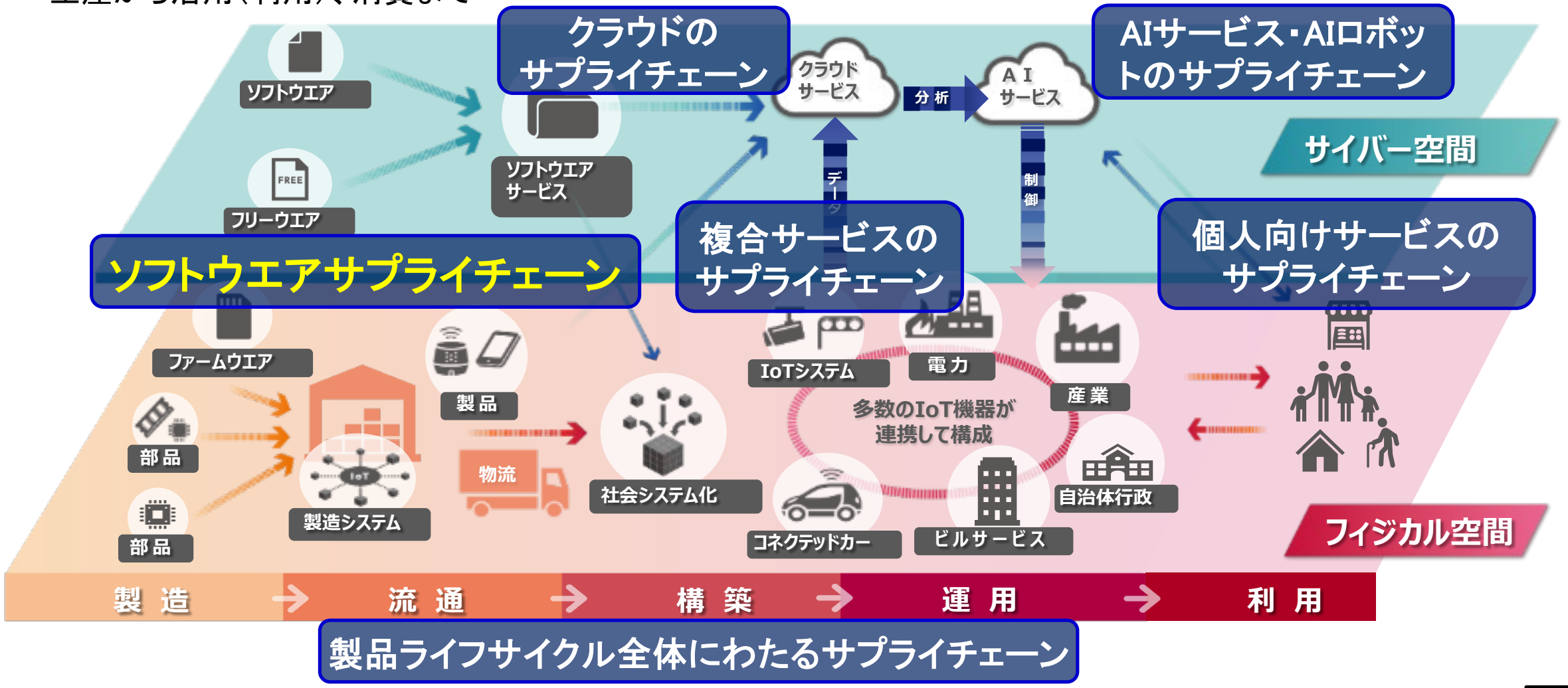
本日の話題提供

- ■サプライチェーンのサイバーリスク （参考事例として）
- ■サイバーセキュリティ確保と偽情報・誤情報対策
  - ●多様な取組の観点
  - ●研究と実務の相互連携と継続性の観点
  - ●データ基盤と大規模LLM基盤の必要性

サプライチェーンのサイバーリスク

サイバー空間とフィジカル空間に跨るサプライチェーン

- 多様なステークホルダー、多様なサプライチェーン
- 生産から活用（利用）、消費まで



ソフトウェアサプライチェーンのセキュリティリスク

⇒セキュリティ確保には透明性向上

■ 3年間で742%の急増（製造業・非製造業・官公庁）

Source: Sonatype社の2023レポート

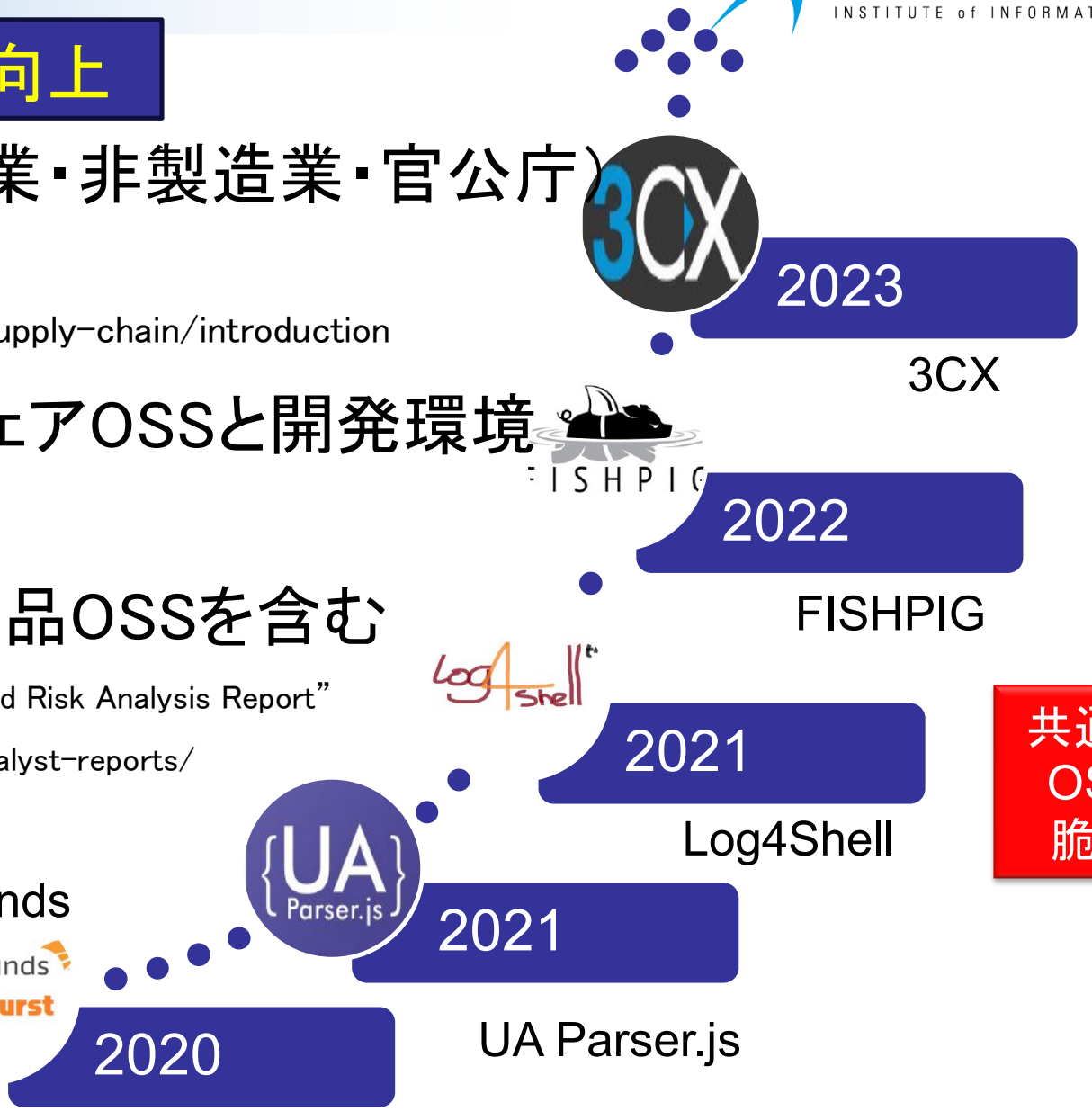
https://www.sonatype.com/state-of-the-software-supply-chain/introduction

■ 特にオープンソースソフトウェアOSSと開発環境に残存する脆弱性

■ ソフトウェアコードの96%は部品OSSを含む

Source: Synopsys社レポート“2023 Open Source Security and Risk Analysis Report”

https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html



ソフトウェアサプライチェーンのセキュリティ確保
～米国政府動向とSBOM（Software Bill of Materials）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

デジタル社会リスクとしての危機感

国家のサイバーセキュリティ改善に係る大統領令（EO14028）2021/5/21

NIST National Institute of Standards and Technology U.S. Department of Commerce

NTIA

- NIST（米国商務省配下の標準技術研究所）が中心となりガイドラインを策定
- ユーザ（調達者）がベンダにSBOM提供を求める動き

- SBOMはソフトウェアの**透明性向上**のための「成分表（≒開発の履歴、来歴管理情報）」

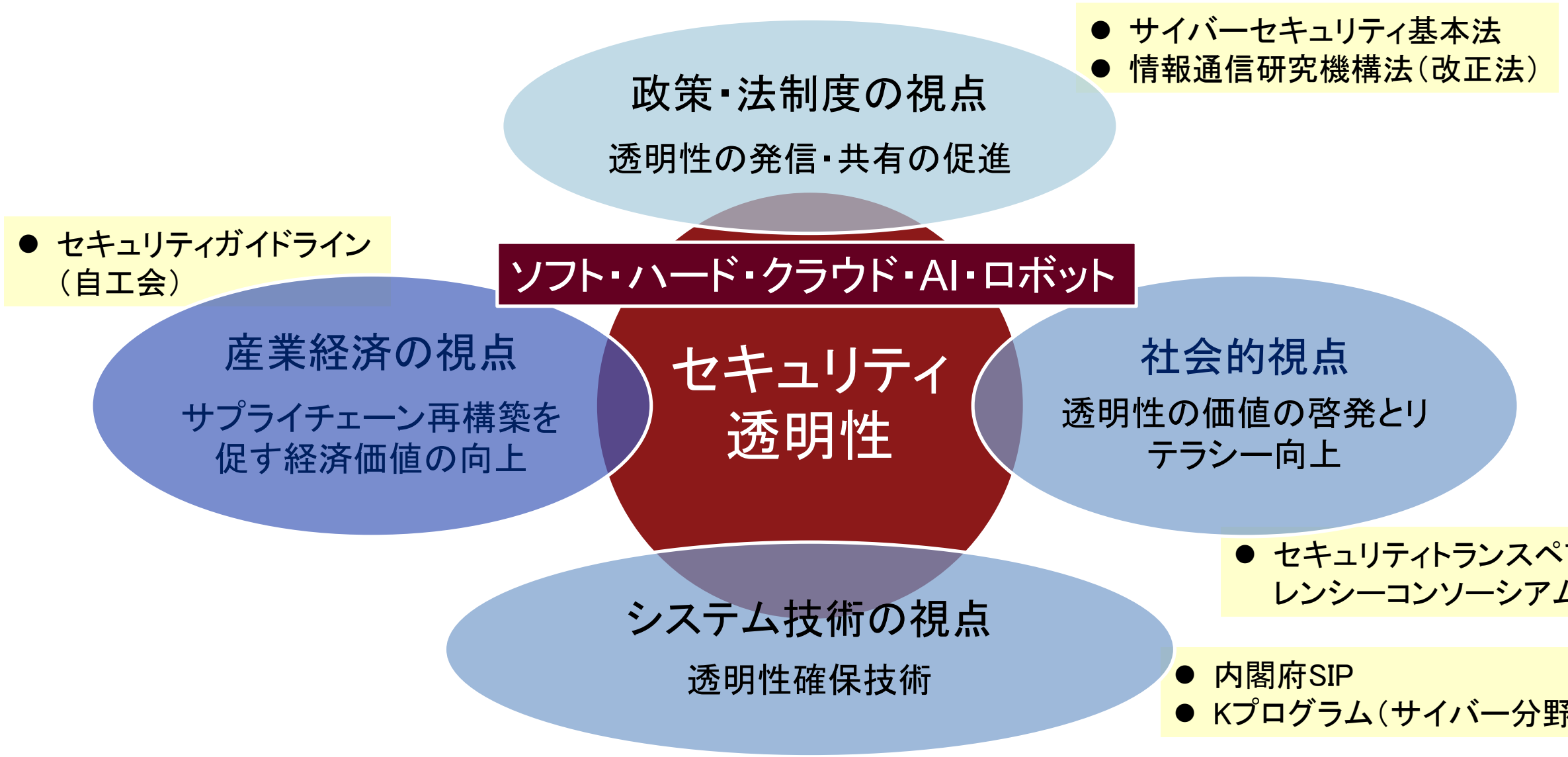
米商務省，NTIA
アラン・フリードマン氏

- 課題：SBOMの用意と管理はコスト高

ベンダーの責務？ ⟺ **コスト負担 v.s. 価値（メリット）の享受**

サプライチェーン全体でのセキュリティ透明性の確保には多様な視点からの取組みが必要

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



多様な取組の観点

ソフトウエアサプライチェーンの
サイバーセキュリティ確保と偽情報・誤情報対策

リスクと背景

情報流通の健全化 偽情報・誤情報対策	リスクと背景	サイバーセキュリティ確保 ソフトウェアサプライチェーン対策
人間の認知機能	直接の対象	コンピュータ・ネットワーク（データ、S/W、H/W） ヒト（騙しの被害者）
社会経済活動のコスト増 災害被害の拡大 選挙妨害・安全保障上の脅威の増加	社会リスク	社会経済活動の停止（直接・波及） 経済的（金銭）被害 安全保障上の脅威の増加
？？	アクター	サイバー犯罪者（集団） 国家レベルの攻撃組織
？？	裏コミュニティ	犯罪者ネットワーク ダークウェブ等のブラックマーケット
アテンションエコノミー （落合先生：デジタル空間における関係者に対する行動インセンティブの設計の課題）	背景課題 （リスクを増長する要因）	ICTサービス・技術の価格競争（低品質システム・ソフトウェア）、人材・技術不足
国民のリテラシーレベル（メディア）と 価値の多様化		国民のリテラシーレベル 先端サービス革新とのギャップ拡大

対策技術・対策手段

情報流通の健全化 偽情報・誤情報対策	対策技術・手段	サイバーセキュリティ確保 ソフトウェアサプライチェーン対策
データ・情報の真贋判定ツール （本質的な「真贋」は判定困難？） 「人」の眼	Check手段	ソフトウェアの真贋判定ツール・マルウェア検出 （過検知、誤検知があることは前提） 参考：NICTER（無差別型サイバー攻撃の観測網）、 NOTICE（脆弱IoT機器調査）等
コンテンツの透明性確保 （OP, CAI, C2IA）	「透明性」 by Design・by Default	ソフトウェアの透明性確保 （ソフトウェア構成情報SBOM）
プラットフォーム事業者？？ メディア？？	確保主体	APサービスベンダー、ソフトウェアベンダー IoT機器、インフラ設備機器の製造ベンダ、事業者
コンテンツモデレーションや レコメンドの透明性確保？ （電子透かし、eシールなどのナリスマシ対策技術？）	確保手段	サプライチェーン、調達・委託の契約 （コスト負担がビジネス上の課題）
ファクトチェック活動？ Trusted News Initiative, IFCN, ？？	（業界としての） 促進策	（自主）業界のコンソーシアム セキュリティ企業等によるコンサルティング
？？	ガイドライン等	経営者ガイドライン、中小企業ガイドライン、 業界毎のガイドライン

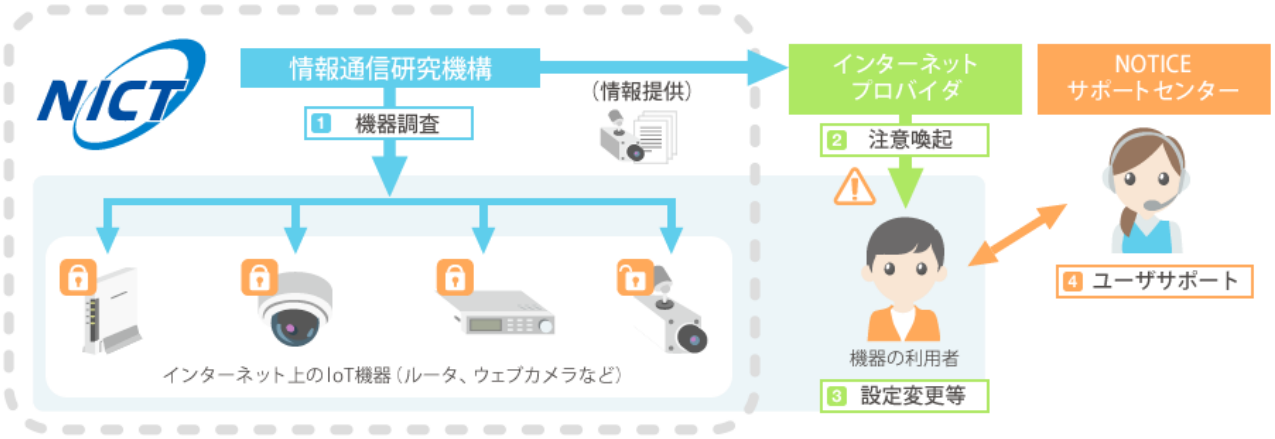
法的な枠組み

情報流通の健全化 偽情報・誤情報対策	法的な枠組み	サイバーセキュリティ確保 ソフトウェアサプライチェーン対策
？？	基本法	サイバーセキュリティ基本法
？？	目的と理念 （多様な主体の連携と積極的対応）	経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現 国際社会の平和及び安全の確保並びに我が国の安全保障に寄与
デジタルプラットフォーム事業者？ 他　？	責務と努力	国・地方公共団体・重要社会基盤事業者・サイバー関連事業者その他の事業者・教育研究機関の責務と国民の努力
？？	戦略と主体	サイバーセキュリティ戦略と サイバーセキュリティ戦略本部
？？*	関連法制度、個別の法制度・省令等	改正NICT法 個人情報保護法　他
国連DPF情報インテグリティ、G7（AI）、IGF、OECD、他	国際法 国際協調・連携	国連憲章、GGE報告書、Secure by Design文書への共同署名、QUAD, AJCCBC　他

*青少年インターネット環境整備法：携帯電話事業者のフィルタリング提供義務等

参考： NOTICEにおけるISP・通信事業者との連携

- NOTICE: 改正されたNICT法に基づくID・パスワードに脆弱性があるIoT機器の調査（特定特定アクセス行為）。NICT、インターネットプロバイダが連携し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査と当該機器の利用者への注意喚起の取組み。
- 2023年12月 NOTICEによる通信機器の調査を延長する改正NICT法成立。ソフトウエア脆弱性も調査対象に。



https://notice.go.jp/

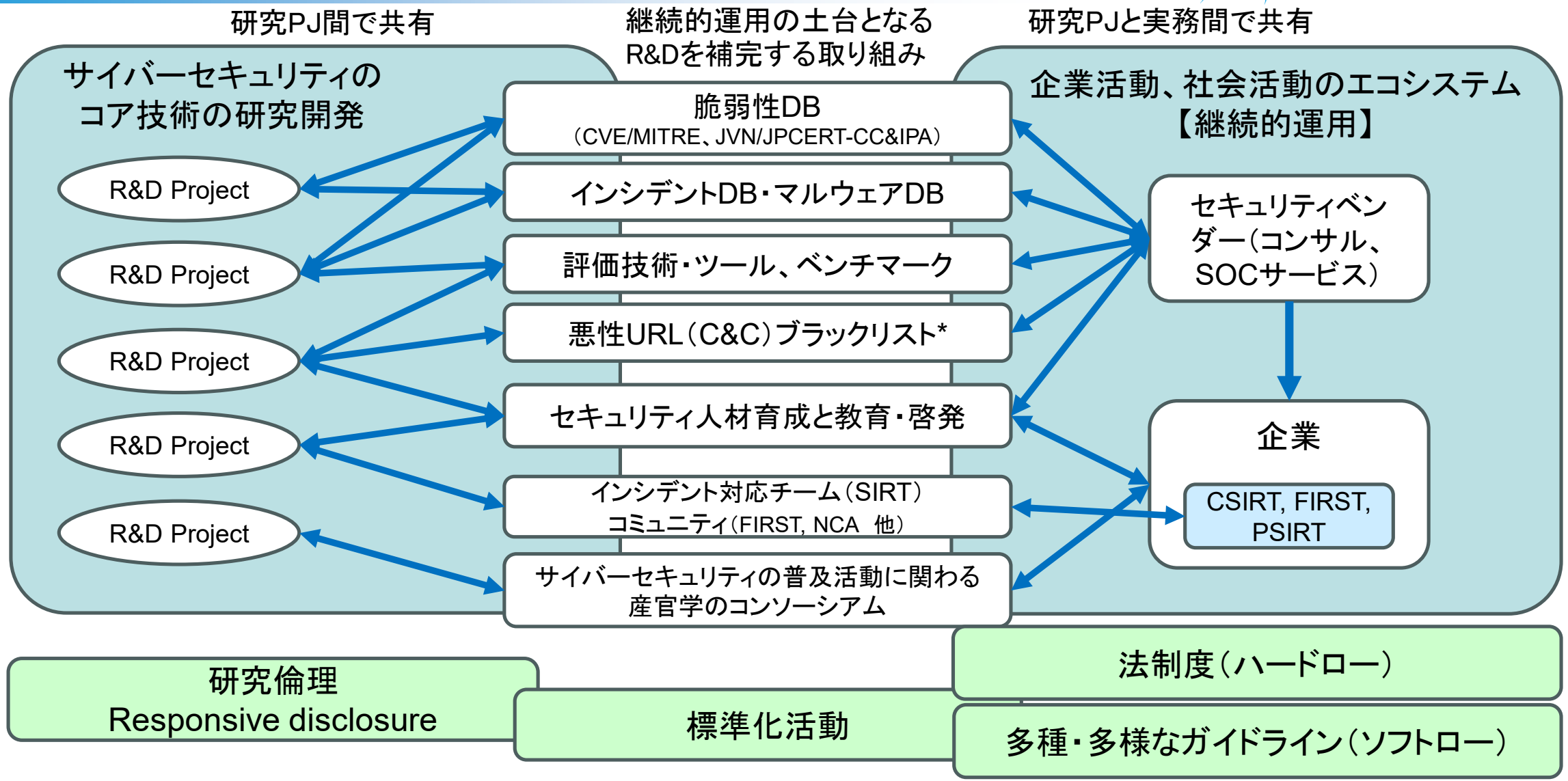
対策技術・手段	NOTICEによるIoTセキュリティ対策
Check手段	インターネット上で外部からアクセスできる脆弱IoT機器調査
法制度	平成30年5月に改正された国立研究開発法人情報通信研究機構法（NICT法）⇒改正法により延長・調査対象拡大
確保主体	NICT・ISP等の通信事業者・NOTICEセンター
確保手段	検出・注意喚起・サポート・ベンダー含む関係事業者への情報共有
促進策	ISP・通信事業者・IoTベンダーによるIoTセキュリティ確保の啓発活動

研究と実務の相互連携と継続性の観点

（ソフトウエアサプライチェーンに限らす幅広く）

サイバーセキュリティ確保と偽情報・誤情報対策

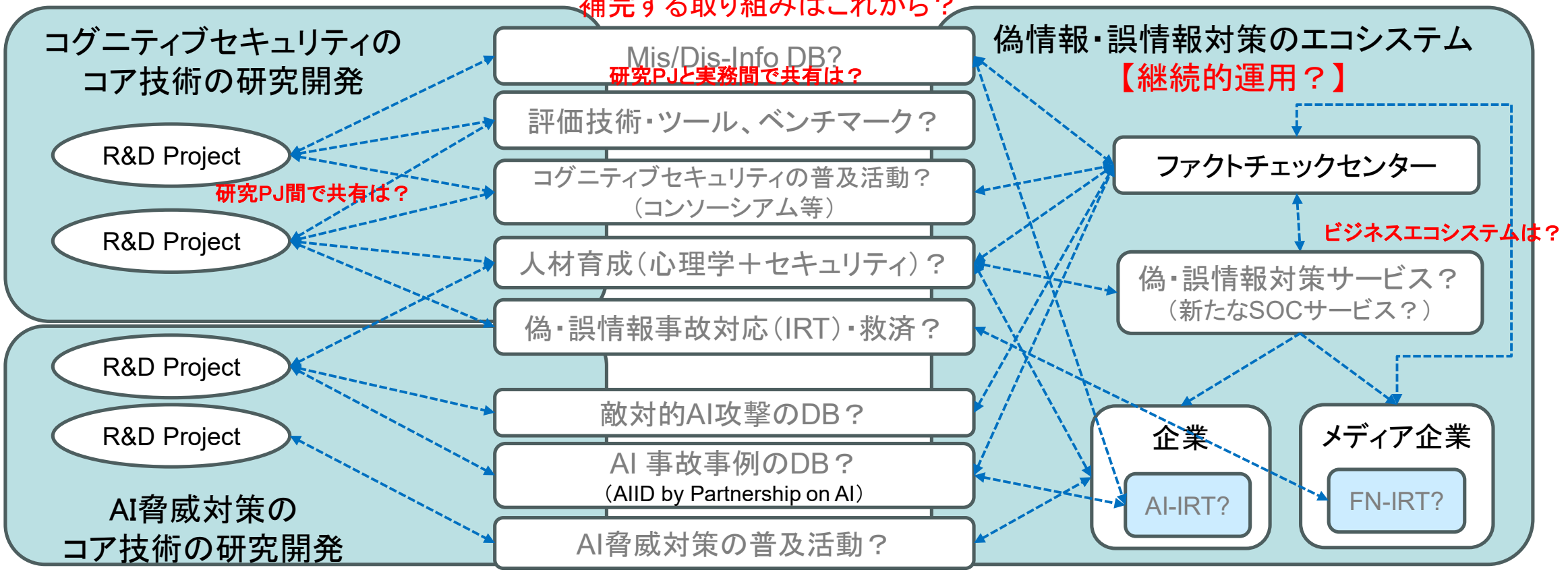
サイバーセキュリティの研究と実務の相互連携と継続性



*C2サーバ検知実証実験では、複数ISPでの検知状況を共有することによって価値が高められるという報告あり

「コグニティブセキュリティ＋AI脅威対策」の研究と実務における相互連携と継続性

継続的運用の土台となるR&Dを
補完する取り組みはこれから？



AI-IRT AI Incident Response Team, FN-IRT Fake News Incident Response Team（後藤の造語）

コグニティブセキュリティ・AI研究倫理

標準化活動？

法制度：AI規制法、個人情報法、他
他に拠り所となる法制度は？

メディア倫理、AI事業者ガイドライン（案）
偽・誤情報ガイドライン？

データ基盤と大規模LLM基盤の必要性

サイバーセキュリティ確保と偽情報・誤情報対策

データ基盤と大規模LLM基盤の必要性

■ 偽情報分析に係る技術の開発（偽情報検知技術、偽情報評価技術 ＝ファクトチェックの前処理？）

- 高信頼データ基盤 with AI分析

  ⇒ 多様なステークホルダー、SNSからの公開情報の（準）リアルタイム収集・検知・評価

  - 検知評価技術の社会実装組織が情報源と契約ベースでデータを入手と想定した場合、その契約条件を満たす高信頼データ基盤が必要（高信頼クラウド？）

  ⇒ AI分析基盤（大規模LLM）

  - 検知評価技術の社会実装組織は大規模LLMベースのAI基盤をどのように確保するか？

- （AI）分析基盤の能力限界が出た事例

  ◆2016年米国大統領選挙におけるSocialBot分析（偽誤情報の影響分析）では、大量のTweetデータを収集して分析
  ⇒ 分析システムの処理能力の限界により、実際にはサンプリングデータで分析

  ◆他、昨今、検知技術や評価技術の研究が盛んになってきているが、大学等では大規模データが扱いきれいない状況

- 同様の分析基盤、データ基盤は広くサイバーセキュリティの研究開発にとっても重要

データ基盤とAI分析基盤（大規模LLM）

コア技術の
R&D

AIを活用した偽情報検知

AI攻撃技術の分析、等

大規模LLM基盤
（AI基盤）

高信頼データ基盤

・多様なステークホルダからの情報（世界のニュース映像のフルダンプなど、の他

（社会実装＝）継続的な運用に求められるもの

まとめ

■ サイバーセキュリティ確保と偽情報・誤情報対策

- 多様な取組の観点

  ➜新設WGによる「法的な枠組みの考え方」の整理を期待（c.f. サイバーセキュリティ基本法）

  ➜幅広く偽情報・誤情報対策の取組みを国内外から収集して広く共有・周知

  ➜NOTICEでのNICT・ISP等の通信事業者、関係事業者の連携の枠組みが参考になるのではないか

- 研究と実務の相互連携と継続性の観点

  ➜複数の研究コミュニティ（研究PJ）が相互に共有できる様々なDBの構築・運用

  ➜上記のDBを研究コミュニティと実務組織で双方向に活用し、継続的に運用

  ➜理論系、技術系、人文系の複数分野にまたがる研究・実務人材の育成

  ➜（CISO、CSIRT、SOCに類する）偽情報・誤情報対応人材・チーム・組織の考え方から実装への取組み

- データ基盤と大規模LLM基盤の必要性

  ➜研究開発から実務までをわが国として自律的に支えるためのデータ基盤＆大規模LLM基盤の整備